

A CARLITZ MODULE ANALOGUE OF THE GRUNWALD–WANG THEOREM

NGUYEN NGOC DONG QUAN

CONTENTS

1. Introduction	1
2. The splitting field of the polynomial $C_a(x) - m$	3
3. An analogue of the Grunwald–Wang theorem for certain Galois extensions \mathbb{K}/k	8
References	11

1. INTRODUCTION

The classical Grunwald–Wang theorem is an example of a local–global (or Hasse) principle stating that except in some *special* cases which are precisely determined, an element m in a number field \mathbb{K} is an a -th power in \mathbb{K} if and only if it is an a -th power in the completion \mathbb{K}_{\wp} of \mathbb{K} for all but finitely many primes \wp of \mathbb{K} . In more concrete terms, the equation $x^a = m$ has a solution $x_{\mathbb{K}}$ in \mathbb{K} if and only if it has a solution x_{\wp} in the completion \mathbb{K}_{\wp} for all but finitely many primes \wp of \mathbb{K} . The aim of this article is to prove a Carlitz module analogue of the Grunwald–Wang theorem.

Throughout the paper, let $A = \mathbb{F}_q[T]$, $k = \mathbb{F}_q(T)$, where q is a power of a prime p , and let $k^{\mathbf{alg}}$ be the algebraic closure of k . Let τ be the map defined by $\tau(x) = x^q$. Let $k\langle\tau\rangle$ denote the twisted polynomial ring equipped with twisted multiplication, namely, $\tau a = a^q \tau$ for all $a \in k$. Let C be the Carlitz module, i.e., $C : A \rightarrow k\langle\tau\rangle$ be an \mathbb{F}_q -algebra homomorphism such that $C_T = T + \tau$. Note that for every commutative k -algebra \mathbf{D} , the action of $\sum_j a_i \tau^j \in k\langle\tau\rangle$ on an element $d \in \mathbf{D}$ is defined by

$$\left(\sum_j a_i \tau^j\right)(d) = \sum_j a_i d^{q^j}.$$

A special case of an analogue of the Grunwald–Wang theorem for function fields was proved by G.-J. van der Heiden [11]. We now describe the result of van der Heiden. Let \mathcal{X} be a projective, smooth, geometrically irreducible curve over the finite field \mathbb{F}_q , and let ∞ be a fixed closed point on \mathcal{X} . Let $\mathbb{F}_q(\mathcal{X})$ be the function field of \mathcal{X} , and let $\mathcal{O}_{\mathbb{F}_q(\mathcal{X})}$ be the ring of functions in $\mathbb{F}_q(\mathcal{X})$ that are regular outside ∞ . Let \mathcal{K} be a finite separable extension of $\mathbb{F}_q(\mathcal{X})$, and let $\iota : \mathcal{O}_{\mathbb{F}_q(\mathcal{X})} \rightarrow \mathcal{K}$ be the natural embedding of $\mathcal{O}_{\mathbb{F}_q(\mathcal{X})}$ into \mathcal{K} . Let $\mathbf{DR} : \mathcal{O}_{\mathbb{F}_q(\mathcal{X})} \rightarrow \mathcal{K}\langle\tau\rangle$ be a Drinfeld module over \mathcal{K} of rank 1, that is, \mathbf{DR} is an \mathbb{F}_q -algebra homomorphism such that for all $f \in \mathcal{O}_{\mathbb{F}_q(\mathcal{X})}$, we have

$$\mathbf{DR}_f = \sum_{j=0}^{\deg(f)} f_j \tau^j,$$

where the f_i are elements in \mathcal{K} with $f_{\deg(f)} \in \mathcal{K}^{\times}$ and $f_0 = \iota(f)$. In [11], Van der Heiden proved the following result.

Theorem 1.1. (*van der Heiden*, [11, Proposition 5])

Let P be a prime element of $\mathcal{O}_{\mathbb{F}_q(\mathcal{X})}$, and let m be an element in \mathcal{K} . Then the equation $\mathbf{DR}_P(x) = m$ has a solution $x_{\mathcal{K}}$ in \mathcal{K} if and only if it has a solution x_{\wp} in the completion \mathcal{K}_{\wp} for every place \wp of \mathcal{K} .

Since P is a prime element of $\mathcal{O}_{\mathbb{F}_q(\mathcal{X})}$ and the equation $\mathbf{DR}_P(x) = m$ in Theorem 1.1 is considered over the field of definition of \mathbf{DR} , namely \mathcal{K} , we see that Theorem 1.1 might be viewed as analogous to the following special case of the classical Grunwald–Wang theorem: *the equation $x^p = m$ with prime p in \mathbb{Z} and $m \in \mathbb{Q}$ has a solution $x_{\mathbb{Q}}$ in \mathbb{Q} if and only if it has a solution x_l in the l -adic field \mathbb{Q}_l for every prime l .*

To better understand the analogies between Theorem 1.1 and the above statement, one can consider the case when $\mathcal{X} = \mathbb{P}_1/\mathbb{F}_q$. Thus $\mathcal{K} = k$, $\mathcal{O}_{\mathbb{F}_q(\mathcal{X})} = A$, and the Drinfeld module \mathbf{DR} is the Carlitz module C that was introduced earlier. There are well-known analogies [1] [2] [3] [9] [10] between the map $x \mapsto x^a$ with $a \in \mathbb{Z}$ and the map $x \mapsto C_a(x)$ with $a \in A$; for example, adjoining torsion points of the Carlitz module to the field k generates cyclotomic function fields in a similar manner as cyclotomic extensions of \mathbb{Q} obtained by adjoining roots of unity to \mathbb{Q} . Hence Theorem 1.1 can be regarded as a special case of the classical Grunwald–Wang theorem.

In the hope of obtaining the best possible analogy with the classical Grunwald–Wang theorem, we will have to be content with working with the Carlitz module over k because, among other reasons, the ring $\mathcal{O}_{\mathbb{F}_q(\mathcal{X})}$ might have non-principal ideals and the analogies between (A, k) and (\mathbb{Z}, \mathbb{Q}) are stronger. It is natural to search for a generalization of Theorem 1.1 that might be viewed as the full Grunwald–Wang theorem in the function field setting.

Question 1.2. *Let \mathbb{K} be a finite separable extension of k . Let a be an element in A of positive degree, and let m be an element of \mathbb{K} . Consider the equation*

$$C_a(x) = m.$$

If $C_a(x) = m$ has a solution x_{\wp} in the completion \mathbb{K}_{\wp} for all but finitely many primes \wp of \mathbb{K} , is it true that the equation $C_a(x) = m$ has a solution $x_{\mathbb{K}}$ in \mathbb{K} ?

An affirmative answer to Question 1.2 should give rise to a result that is analogous to the classical Grunwald–Wang theorem in the number field case, and is a generalization of the result of van der Heiden in the Carlitz module setting. Indeed, in contrast to Theorem 1.1, although the field of definition of the Carlitz module is k , we consider the equation $C_a(x) = m$ over any finite separable extension of k . Furthermore a can be any element in A of positive degree, and we *only* require that the equation $C_a(x) = m$ is locally solvable at *all but finitely many primes* of \mathbb{K} . In comparison with the number field case, the classical Grunwald–Wang theorem considers global solvability of the equation $x^a = m$ over a number field although the power map x^a with $a \in \mathbb{Z}$ is defined over \mathbb{Q} .

Let $\Lambda_a \subset k^{\mathbf{alg}}$ be the cyclic A -module defined by $\Lambda_a = \{\lambda \in k^{\mathbf{alg}} \mid C_a(x) = 0\}$. The following theorem is a summary of the main results in this paper.

Theorem 1.3. *Question 1.2 has an affirmative answer in the following cases:*

- (i) \mathbb{K} contains a primitive generator of the cyclic A -module Λ_a .
- (ii) \mathbb{K} is a Galois extension of k such that every prime P dividing a is unramified in \mathbb{K} .

Part (i) of Theorem 1.3 is the content of Corollary 2.8, and part (ii) is the content of Theorem 3.1. Note that Theorem 3.1 and Corollary 2.8 actually are more general than Theorem 1.3. More precisely, in the statements of Theorem 3.1 and Corollary 2.8, instead of assuming local solvability of the equation $C_a(x) = m$ at almost all primes in \mathbb{K} , we only assume that $C_a(x) = m$ has a solution x_{\wp} in the completion \mathbb{K}_{\wp} for all primes \wp in a set of primes of \mathbb{K} of Dirichlet density greater than $1 - 1/\phi(a)q^{\deg(a)}$. Here $\phi(a)$ is the function field analogue of the Euler ϕ -function.

Let us say a few words about the ideas of the proof of Theorem 1.3. In [7], T. Ono and T. Terasoma attempted to give a different proof of a special case of the classical Grunwald–Wang theorem. Unfortunately the statement of a special case of the Grunwald–Wang theorem as well as its attempted proof given in [7] were erroneous as pointed out by T. Ono [8]. Despite the errors in [7], the underlying ideas in that paper can be modified to apply to the function field setting. We will carry out such modifications in the proof of Theorem 1.3 whose main ingredients are the use of Tchebotarev density theorem and basic facts in class field theory over function fields. Thus the ideas of this paper are completely different from those used in [11] in which G.-J. van der Heiden extensively used Galois cohomology.

2. THE SPLITTING FIELD OF THE POLYNOMIAL $C_a(x) - m$

Let \mathbb{K} be a finite, separable extension of k . Let a be an element in A , and let m be an element in \mathbb{K} . In this section, we will describe the splitting field of the polynomial $C_a(x) - m \in \mathbb{K}[x]$ over \mathbb{K} when the equation $C_a(x) = m$ is locally solvable at all primes in a set of primes of \mathbb{K} of Dirichlet density greater than $1 - 1/\phi(a)q^{\deg(a)}$. The case that the equation $C_a(x) = m$ has a solution x_\wp in \mathbb{K}_\wp for almost all primes in \mathbb{K} follows immediately as a special case. The following result is very elementary and can be derived from the results in [9, Chapter 12]. For the sake of self-containedness, we also include a proof here.

Lemma 2.1. *Let a be a polynomial of positive degree s in A . Let $\Lambda_a \subset k^{\text{alg}}$ be the A -module defined by*

$$\Lambda_a = \{\lambda \in k^{\text{alg}} \mid C_a(\lambda) = 0\},$$

and let λ_a be a generator for the cyclic A -module Λ_a (see [9, Chapter 12]). Then

- (i) $C_b(\lambda_a) \neq C_c(\lambda_a)$ for every $b, c \in A$ with $b \neq c$ and $\max(\deg(b), \deg(c)) < s$; and
- (ii) $\Lambda_a = \{C_b(\lambda_a) \mid b \in A \text{ with } \deg(b) < s\}$.

Proof. Part (ii) follows immediately from part (i). We now prove part (i). Let b, c be distinct elements in A with $\max(\deg(b), \deg(c)) < s$. Assume that $C_b(\lambda_a) = C_c(\lambda_a)$. It then follows that

$$C_{b-c}(\lambda_a) = 0.$$

Since $b \neq c$, we see that $b - c \neq 0$, and hence $0 \leq \deg(b - c) < s$. If $\deg(b - c) = 0$, we see that $b - c$ belongs to \mathbb{F}_q^\times , and hence $C_{b-c}(\lambda_a) = (b - c)\lambda_a = 0$. Thus $\lambda_a = 0$, which is a contradiction.

If $\deg(b - c) > 0$, we know from [9, Proposition 12.4] that Λ_{b-c} has exactly $q^{\deg(b-c)}$ elements. Since $C_{b-c}(\lambda_a) = 0$ and λ_a is a generator of the A -module Λ_a , we deduce that $\Lambda_a \subseteq \Lambda_{b-c}$. Thus

$$q^s = q^{\deg(a)} = \#\Lambda_a \leq \#\Lambda_{b-c} = q^{\deg(b-c)},$$

and therefore $s \leq \deg(b - c)$, which is a contradiction. Therefore $C_b(\lambda_a) \neq C_c(\lambda_a)$. □

We now prove the main result in this section.

Theorem 2.2. *Let \mathbb{K} be a finite, separable extension of k . Let m be an element in \mathbb{K} , and let a be a polynomial of positive degree in A . Let \mathbb{L} be the splitting field of the polynomial $C_a(x) - m \in \mathbb{K}[x]$ over \mathbb{K} . Let λ_a be a generator of the A -module Λ_a , where*

$$\Lambda_a = \{\lambda \in k^{\text{alg}} \mid C_a(\lambda) = m\}.$$

Assume that the equation $C_a(x) = m$ has a solution x_\wp in the completion \mathbb{K}_\wp for all but finitely many primes \wp of \mathbb{K} . Then $\mathbb{L} = \mathbb{K}(\lambda_a)$.

Proof. Note that $\mathbb{K} \subset k^{\text{alg}}$ since \mathbb{K} is a finite extension of k . Let h be an element in k^{alg} such that

$$C_a(h) = m.$$

By Lemma 2.1, we see that the set of all solutions of the equation $C_a(x) = m$ is given by

$$(1) \quad \mathcal{S} = \{C_b(\lambda_a) + h \mid b \in A \text{ with } \deg(b) < \deg(a)\}.$$

Since the polynomial $C_a(x) - m$ is separable and \mathbb{L} is the splitting field of the polynomial $C_a(x) - m \in \mathbb{K}[x]$, we deduce that $\mathbb{L} = \mathbb{K}(\mathcal{S})$ and \mathbb{L} is a Galois extension of \mathbb{K} . Since $\lambda_a = (C_1(\lambda_a) + h) - (C_0(\lambda_a) + h)$, we see that $\lambda_a \in \mathbb{L}$. We see that $h = C_0(\lambda) + h \in \mathbb{L}$, and thus

$$\mathbb{L} = \mathbb{K}(\lambda_a, h).$$

Let $\text{Gal}(\mathbb{L}/\mathbb{K})$ denote the Galois group of the Galois extension \mathbb{L}/\mathbb{K} . An element $\psi \in \text{Gal}(\mathbb{L}/\mathbb{K})$ is uniquely determined by its action on λ_a and h . Hence to each element $\psi \in \text{Gal}(\mathbb{L}/\mathbb{K})$, we can associate

a unique ordered pair $(b_\psi, u_\psi) \in (A/aA)^\times \times A/aA$ such that $\psi(\lambda_a) = C_{b_\psi}(\lambda_a)$ and $\psi(h) = C_{u_\psi}(\lambda_a) + h$. Let $\Psi : \text{Gal}(\mathbb{L}/\mathbb{K}) \rightarrow \text{GL}_2(A/aA)$ be the map defined by

$$(2) \quad \Psi(\psi) = \begin{pmatrix} b_\psi & u_\psi \\ 0 & 1 \end{pmatrix}$$

for each $\psi \in \text{Gal}(\mathbb{L}/\mathbb{K})$. Since C is the Carlitz module, it is not difficult to see that for any elements $\sigma, \psi \in \text{Gal}(\mathbb{L}/\mathbb{K})$, the action of $\psi \circ \sigma$ on λ_a and h are given by

$$(\psi \circ \sigma)(\lambda_a) = C_{b_\psi b_\sigma}(\lambda_a) \quad \text{and} \quad (\psi \circ \sigma)(h) = C_{b_\psi u_\sigma + u_\psi}(\lambda_a) + h,$$

where $(b_\sigma, u_\sigma), (b_\psi, u_\psi) \in (A/aA)^\times \times A/aA$ are uniquely determined by σ, ψ , respectively in the same way as above. Hence Ψ is an injective homomorphism.

Let Σ be the image of $\text{Gal}(\mathbb{L}/\mathbb{K})$ under Ψ . Set

$$(3) \quad \mathcal{E} = \left\{ \begin{pmatrix} \star & \star \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(A/aA) \right\}$$

and

$$(4) \quad \mathcal{M} = \left\{ \begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(A/aA) \right\}.$$

We see that Σ is a subgroup of \mathcal{E} and $\mathcal{E}/\mathcal{M} \cong (A/aA)^\times$. Hence we obtain the embedding

$$(5) \quad \Sigma/\Sigma \cap \mathcal{M} \hookrightarrow \mathcal{E}/\mathcal{M} \cong (A/aA)^\times.$$

We contend that $\Sigma \cap \mathcal{M} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. Indeed, let $M = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ be an arbitrary element in $\Sigma \cap \mathcal{M}$ for some element $u \in A/aA$. Then there exists an element $\psi \in \text{Gal}(\mathbb{L}/\mathbb{K})$ such that $\Psi(\psi) = M$. Let $(b_\psi, u_\psi) \in (A/aA)^\times \times (A/aA)$ be the ordered pair uniquely determined by

$$(6) \quad \psi(\lambda_a) = C_{b_\psi}(\lambda_a)$$

and

$$(7) \quad \psi(h) = C_{u_\psi}(\lambda_a) + h.$$

By the definition of Ψ , we see that

$$\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} = M = \Psi(\psi) = \begin{pmatrix} b_\psi & u_\psi \\ 0 & 1 \end{pmatrix},$$

and it thus follows that

$$(8) \quad b_\psi = 1$$

and

$$(9) \quad u_\psi = u.$$

By assumption, we know that there exists a finite set of primes of \mathbb{K} , say, \mathcal{P} such that $C_a(x) = m$ has a solution x_\wp in the completion \mathbb{K}_\wp for every prime \wp of \mathbb{K} with $\wp \notin \mathcal{P}$.

By the Tchebotarev density theorem (see [9, Theorem 9.13A]), there exist infinitely many primes \wp in \mathbb{K} such that \wp is unramified in \mathbb{L} and ψ is equal to the Frobenius automorphism $(\mathfrak{B}, \mathbb{L}/\mathbb{K})$ for some prime \mathfrak{B} in \mathbb{L} lying above \wp . Since the set \mathcal{P} is finite, one can choose a prime \wp in \mathbb{K} with $\wp \notin \mathcal{P}$ such that \wp is unramified in \mathbb{L} and $\psi = (\mathfrak{B}, \mathbb{L}/\mathbb{K})$ for some prime \mathfrak{B} in \mathbb{L} lying above \wp .

Let $\mathcal{D}(\mathfrak{B}/\wp)$ be the decomposition group of \mathfrak{B} over \wp . It is well-known [6, Proposition 9.8] that the fixed field of $\mathcal{D}(\mathfrak{B}/\wp)$, or equivalently the decomposition field of \mathfrak{B} over \wp , is $\mathbb{L} \cap \mathbb{K}_\wp$. Since $\wp \notin \mathcal{P}$, we know that there exists an element x_\wp in \mathbb{K}_\wp such that $C_a(x_\wp) = m$. Hence x_\wp belongs to \mathcal{S} , where \mathcal{S} is given by (1). Thus $x_\wp = C_b(\lambda_a) + h$ for some $b \in A$ with $\deg(b) < \deg(a)$. In particular this implies that $x_\wp \in \mathbb{L} \cap \mathbb{K}_\wp$.

Since $\psi = (\mathfrak{B}, \mathbb{L}/\mathbb{K}) \in \mathcal{D}(\mathfrak{B}/\wp)$ and $\mathbb{L} \cap \mathbb{K}_\wp$ is the fixed field of $\mathcal{D}(\mathfrak{B}/\wp)$, we deduce that

$$\psi(x_\wp) = (\mathfrak{B}, \mathbb{L}/\mathbb{K})(x_\wp) = x_\wp.$$

On the other hand, we deduce from (8) and (9) that

$$\begin{aligned}
C_b(\lambda_a) + h = x_\wp &= \psi(x_\wp) = \psi(C_b(\lambda_a) + h) \\
&= \psi(C_b(\lambda_a)) + \psi(h) \\
&= C_b(\psi(\lambda_a)) + C_u(\lambda) + h \\
&= C_b(C_1(\lambda_a)) + C_u(\lambda) + h \\
&= C_b(\lambda_a) + C_u(\lambda) + h,
\end{aligned}$$

and thus $C_u(\lambda_a) = 0$.

If $u \neq 0$, then we deduce from Lemma 2.1 that $C_u(\lambda_a) \neq C_0(\lambda_a)$, and thus $C_u(\lambda_a) \neq 0$, which is a contradiction. Therefore $u = 0$, and hence

$$(10) \quad \Sigma \cap \mathcal{M} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Let \mathbf{I} be the subgroup of $\text{Gal}(\mathbb{L}/\mathbb{K})$ that corresponds to the subfield $\mathbb{K}(\lambda_a)$ of \mathbb{L} . In other words, $\mathbb{K}(\lambda_a)$ is the fixed field of \mathbf{I} . Take any element $\sigma \in \mathbf{I}$. We know that there exists a unique ordered pair $(b_\sigma, u_\sigma) \in (A/aA)^\times \times A/aA$ such that $\sigma(\lambda_a) = C_{b_\sigma}(\lambda_a)$ and $\sigma(h) = C_{u_\sigma}(\lambda_a) + h$. Since σ belongs to \mathbf{I} , we know that $C_{b_\sigma}(\lambda_a) = \sigma(\lambda_a) = \lambda_a = C_1(\lambda_a)$, and it thus follows from Lemma 2.1 that $b_\sigma = 1$. Hence we deduce that

$$\Psi(\sigma) = \begin{pmatrix} b_\sigma & u_\sigma \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & u_\sigma \\ 0 & 1 \end{pmatrix},$$

and hence $\Psi(\sigma) \in \Sigma \cap \mathcal{M}$. By (10), we deduce that $\Psi(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and thus $u_\sigma = 0$. Hence σ is the identity map, and therefore $\mathbf{I} = \{\text{id}_\mathbb{L}\}$. Thus by Galois theory, we deduce that $\mathbb{L} = \mathbb{K}(\lambda_a)$, which proves our contention. \square

Remark 2.3. One of the key ingredients in proving Theorem 2.2 is the use of Tchebotarev density theorem to prove that $\Sigma \cap \mathcal{M} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. For an element $\psi \in \text{Gal}(\mathbb{L}/\mathbb{K})$, if we use the precise formula for the Dirichlet density of all unramified primes \mathfrak{p} in \mathbb{K} such that the set $(\mathfrak{p}, \mathbb{L}/\mathbb{K})$ of all Frobenius automorphisms equals the conjugacy class of ψ in $\text{Gal}(\mathbb{L}/\mathbb{K})$, then we obtain a stronger result than Theorem 2.2. We will shortly prove a refinement of Theorem 2.2 using the Dirichlet density that leads us to the same conclusion as Theorem 2.2 with less *restrictive* assumptions.

Let us first recall some basic notions and the precise statement of Tchebotarev density theorem as presented in [9, Chapter 9]. Let \mathbb{L}/\mathbb{K} be a Galois extension of global function fields. Let $\mathcal{P}_\mathbb{K}$ be the set of all primes in \mathbb{K} , and let \mathcal{A} be a set of primes of \mathbb{K} . If the limit given by

$$(11) \quad \lim_{s \rightarrow 1^+} \frac{\sum_{\wp \in \mathcal{A}} N\wp^{-s}}{\sum_{\wp \in \mathcal{P}_\mathbb{K}} N\wp^{-s}}$$

exists, we define the *Dirichlet density* of \mathcal{A} to be the value of the limit given by (11), and denote it by $\delta(\mathcal{A})$. If the limit given by (11) does not exist, we say that \mathcal{A} does not have the Dirichlet density.

We now recall the statement of Tchebotarev density theorem.

Theorem 2.4. (see [9, Theorem 9.13A])

Let \mathbb{L}/\mathbb{K} be a Galois extension of global function fields, and let $\text{Gal}(\mathbb{L}/\mathbb{K})$ denote the Galois group. Let $\mathcal{P}_\mathbb{K}^{un}$ be the set of primes of \mathbb{K} that are unramified in \mathbb{L} . Let $\mathbf{C} \subset \text{Gal}(\mathbb{L}/\mathbb{K})$ be a conjugacy class in $\text{Gal}(\mathbb{L}/\mathbb{K})$. Let \mathcal{H} be the subset of $\mathcal{P}_\mathbb{K}^{un}$ defined by

$$\mathcal{H} = \{ \wp \in \mathcal{P}_\mathbb{K}^{un} \mid (\wp, \mathbb{L}/\mathbb{K}) = \mathbf{C} \}.$$

Then

$$\delta(\mathcal{H}) = \frac{\text{Card}(\mathbf{C})}{\text{Card}(\text{Gal}(\mathbb{L}/\mathbb{K}))},$$

where $\mathbf{Card}(\cdot)$ denotes the number of elements in a set (\cdot) .

We now prove a refinement of Theorem 2.2 in which we only assume that the equation $C_a(x) = m$ is locally solvable at all primes \wp in a set of the Dirichlet density greater than $1 - 1/\mathbf{Card}(\text{Gal}(\mathbb{L}/\mathbb{K}))$.

Theorem 2.5. *We maintain the same notation as in Theorem 2.2. Let \mathcal{H} be a set of primes in \mathbb{K} such that the Dirichlet density of \mathcal{H} satisfies*

$$(12) \quad \delta(\mathcal{H}) > 1 - \frac{1}{\mathbf{Card}(\text{Gal}(\mathbb{L}/\mathbb{K}))}.$$

Assume that the equation $C_a(x) = m$ has a solution x_\wp in the completion \mathbb{K}_\wp for each prime $\wp \in \mathcal{H}$. Then $\mathbb{L} = \mathbb{K}(\lambda_a)$.

Remark 2.6. We can replace the lower bound of $\delta(\mathcal{H})$ in (12) by an absolute lower bound that only depends on a . Indeed, following the first part of the proof of Theorem 2.2, we know that $\mathbb{L} = \mathbb{K}(\lambda_a, h)$. Note that this follows directly from the fact that \mathbb{L} is the splitting field of the polynomial $C_a(x) - m \in \mathbb{K}[x]$ over \mathbb{K} . By [12, Theorem 12.3.16], we know that λ_a is a root of the a -th cyclotomic polynomial $\Phi_a(x) \in k[x] \subset \mathbb{K}[x]$. We also know from [12, Theorem 12.3.16] that the degree of $\Phi_a(x)$ is $\phi(a)$, where $\phi(a)$ is the number of nonzero polynomials in A of degree less than $\deg(a)$ and relatively prime to a . (For a precise formula for $\phi(a)$, see [9, Proposition 1.7].) Thus

$$[\mathbb{K}(\lambda_a) : \mathbb{K}] \leq \phi(a).$$

Since the polynomial $C_a(x) - m \in \mathbb{K}[x]$ is of degree $q^{\deg(a)}$ and $C_a(h) = m$, we deduce that

$$[\mathbb{L} : \mathbb{K}(\lambda_a)] = [\mathbb{K}(\lambda_a)(h) : \mathbb{K}(\lambda_a)] \leq \deg(C_a(x) - m) = q^{\deg(a)},$$

and therefore

$$\mathbf{Card}(\text{Gal}(\mathbb{L}/\mathbb{K})) = [\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}(\lambda_a)][\mathbb{K}(\lambda_a) : \mathbb{K}] \leq \phi(a)q^{\deg(a)}.$$

Thus

$$1 - \frac{1}{\mathbf{Card}(\text{Gal}(\mathbb{L}/\mathbb{K}))} \leq 1 - \frac{1}{\phi(a)q^{\deg(a)}}.$$

We see from the above inequality that if $\delta(\mathcal{H}) > 1 - \frac{1}{\phi(a)q^{\deg(a)}}$, then the condition (12) follows trivially.

Proof of Theorem 2.5. We maintain the same notation as in the proof of Theorem 2.2. As noted in Remark 2.3, a crucial ingredient in the proof of Theorem 2.2 is the use of Tchebotarev density theorem to prove that

$$(13) \quad \Sigma \cap \mathcal{M} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Looking closely at the proof of Theorem 2.2, we see that once we establish (13), then it follows immediately that $\mathbb{L} = \mathbb{K}(\lambda_a)$. Hence it suffices to verify (13).

Take any element $M = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in \Sigma \cap \mathcal{M}$ for some $u \in A/aA$. There exists an element $\psi \in \text{Gal}(\mathbb{L}/\mathbb{K})$ such that $\Psi(\psi) = M = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$, where Ψ is the injective homomorphism defined by (2). Since Ψ is injective, we see from the definition of Ψ that $\psi(\lambda) = C_1(\lambda_a) = \lambda_a$ and $\psi(h) = C_u(\lambda_a) + h$.

Let \mathbf{C}_ψ be the conjugacy class of ψ in $\text{Gal}(\mathbb{L}/\mathbb{K})$. Since $\psi \in \mathbf{C}_\psi$, we see that $\mathbf{Card}(\mathbf{C}_\psi) \geq 1$. Let \mathcal{B}_ψ be the set defined by

$$\mathcal{B}_\psi = \{ \wp \in \mathcal{P}_{\mathbb{K}}^{\text{un}} \mid (\wp, \mathbb{L}/\mathbb{K}) = \mathbf{C}_\psi \},$$

where $\mathcal{P}_{\mathbb{K}}^{\text{un}}$ is the set of all primes of \mathbb{K} that are unramified in \mathbb{L} . We prove that $\mathcal{H} \cap \mathcal{B}_\psi \neq \emptyset$. Assume the contrary, that is, $\mathcal{H} \cap \mathcal{B}_\psi = \emptyset$. Then

$$(14) \quad \delta(\mathcal{H} \cup \mathcal{B}_\psi) = \delta(\mathcal{H}) + \delta(\mathcal{B}_\psi).$$

On the one hand, we see that $\delta(\mathcal{H} \cup \mathcal{B}_\psi) \leq \delta(\mathcal{P}_\mathbb{K}) = 1$, where $\mathcal{P}_\mathbb{K}$ denotes the set of all primes in \mathbb{K} . On the other hand, since $\mathbf{Card}(\mathbf{C}_\psi) \geq 1$, we deduce from Theorem 2.4 that

$$\begin{aligned} \delta(\mathcal{H}) + \delta(\mathcal{B}_\psi) &= \delta(\mathcal{H}) + \frac{\mathbf{Card}(\mathbf{C}_\psi)}{\mathbf{Card}(\mathrm{Gal}(\mathbb{L}/\mathbb{K}))} \\ &> \left(1 - \frac{1}{\mathbf{Card}(\mathrm{Gal}(\mathbb{L}/\mathbb{K}))}\right) + \frac{1}{\mathbf{Card}(\mathrm{Gal}(\mathbb{L}/\mathbb{K}))} \\ &= 1 \geq \delta(\mathcal{H} \cup \mathcal{B}_\psi), \end{aligned}$$

which is a contradiction to (14). Therefore $\mathcal{H} \cap \mathcal{B}_\psi \neq \emptyset$, and it thus follows that there exists a prime \mathfrak{q} in \mathbb{K} such that $\mathfrak{q} \in \mathcal{H}$, \mathfrak{q} is unramified in \mathbb{L} and the Frobenius automorphism $(\mathfrak{B}/\mathfrak{q}, \mathbb{L}/\mathbb{K})$ equals ψ for some prime \mathfrak{B} in \mathbb{L} lying above \mathfrak{q} .

By assumption, we know that there exists an element $x_{\mathfrak{q}}$ in the completion $\mathbb{K}_{\mathfrak{q}}$ of \mathbb{K} such that $C_a(x_{\mathfrak{q}}) = m$. Repeating the same arguments as in the proof of Theorem 2.2, we see that

$$x_{\mathfrak{q}} = (\mathfrak{B}/\mathfrak{q}, \mathbb{L}/\mathbb{K})(x_{\mathfrak{q}}) = \psi(x_{\mathfrak{q}}).$$

From the above equation, one can follow the arguments in the proof of Theorem 2.2 to prove that $C_u(\lambda_a) = 0$, and thus $u = 0$. Therefore (13) holds, and as remarked in the first paragraph of this proof, we deduce immediately that $\mathbb{L} = \mathbb{K}(\lambda_a)$. □

The following result follows immediately from Remark 2.6.

Corollary 2.7. *We maintain the same notation as in Theorem 2.2. Let \mathcal{H} be a set of primes in \mathbb{K} such that the Dirichlet density of \mathcal{H} satisfies*

$$(15) \quad \delta(\mathcal{H}) > 1 - \frac{1}{\phi(a)q^{\deg(a)}}.$$

Assume that the equation $C_a(x) = m$ has a solution x_{\wp} in the completion \mathbb{K}_{\wp} for each prime $\wp \in \mathcal{H}$. Then $\mathbb{L} = \mathbb{K}(\lambda_a)$.

By the above corollary, we obtain a Carlitz module analogue of the Grunwald–Wang theorem in the case that \mathbb{K} contains a generator of the A -module Λ_a .

Corollary 2.8. *We maintain the same notation as in Theorem 2.2. Assume that \mathbb{K} contains a generator λ_{\star} of the module Λ_a . Let \mathcal{H} be a set of primes in \mathbb{K} such that the Dirichlet density of \mathcal{H} satisfies*

$$\delta(\mathcal{H}) > 1 - \frac{1}{\phi(a)q^{\deg(a)}}.$$

Then the equation $C_a(x) = m$ has a solution $x_{\mathbb{K}}$ in \mathbb{K} if and only if it has a solution x_{\wp} in the completion \mathbb{K}_{\wp} of \mathbb{K} for every prime $\wp \in \mathcal{H}$.

Proof. If $C_a(x) = m$ has a solution $x_{\mathbb{K}}$ in \mathbb{K} , then it is obvious that it is locally solvable at every prime of \mathbb{K} .

If $C_a(x) = m$ is locally solvable at every prime in \mathcal{H} , we deduce from Corollary 2.7 that $\mathbb{L} = \mathbb{K}(\lambda_a)$. Since $\lambda_{\star}, \lambda_a$ are generators of Λ_a , it follows that $\mathbb{L} = \mathbb{K}(\lambda_a) = \mathbb{K}(\lambda_{\star}) = \mathbb{K}$. Since \mathbb{L} is the splitting field of the polynomial $C_a(x) - m \in \mathbb{K}[x]$ over \mathbb{K} , we deduce that all solutions to the equation $C_a(x) = m$ belong to \mathbb{K} . □

Remark 2.9. It is known (see [9, Chapter 12]) that a generator of the A -module Λ_a is a function field analogue of a primitive a -th root of unity in the number field setting. It is well-known (see [1], [2], [3], [9], and [10]) that the map $x \mapsto C_a(x)$ with $a \in A$ is a Carlitz module analogue of the map $x \mapsto x^a$ with $a \in \mathbb{Z}$ in the number field setting. Thus Corollary 2.8 is a Carlitz module analogue of the classical Grunwald–Wang theorem in the case that \mathbb{K} contains a generator of the A -module Λ_a . For an account of a similar result in the number field setting, see [5, Theorem 1.1, Chapter VIII].

3. AN ANALOGUE OF THE GRUNWALD–WANG THEOREM FOR CERTAIN GALOIS EXTENSIONS \mathbb{K}/k

In this section, we prove a Carlitz module analogue of the classical Grunwald–Wang theorem for certain Galois extensions \mathbb{K}/k . The following theorem is the main result in this section.

Theorem 3.1. *We maintain the same notation as in Theorem 2.2. Assume that \mathbb{K} is a Galois extension of k such that every prime P dividing a is unramified in \mathbb{L} . Let \mathcal{H} be a set of primes of \mathbb{K} satisfying the following conditions:*

(i) *the Dirichlet density of \mathcal{H} satisfies*

$$\delta(\mathcal{H}) > 1 - \frac{1}{\phi(a)q^{\deg(a)}}; \text{ and}$$

(ii) *\mathcal{H} contains all primes \wp of \mathbb{K} that divides a .*

Then the equation $C_a(x) = m$ has a solution $x_{\mathbb{K}}$ in \mathbb{K} if and only if it has a solution x_{\wp} in the completion \mathbb{K}_{\wp} of \mathbb{K} for every prime \wp of \mathbb{K} with $\wp \in \mathcal{H}$.

Proof. If $C_a(x) = m$ has a solution $x_{\mathbb{K}}$ in \mathbb{K} , then it follows immediately that $C_a(x) = m$ has a solution x_{\wp} in the completion K_{\wp} for every prime \wp in \mathbb{K} .

Suppose that $C_a(x) = m$ has a solution x_{\wp} in the completion \mathbb{K}_{\wp} for each prime $\wp \in \mathcal{H}$. We will prove that the equation $C_a(x) = m$ has a solution $x_{\mathbb{K}} \in \mathbb{K}$.

By assumption, we know from Corollary 2.7 that $\mathbb{L} = \mathbb{K}(\lambda_a)$.

Let h be an element in k^{alg} such that $C_a(h) = m$, and let \mathcal{S} be the set defined by (1) in the proof of Theorem 2.2. Since a is a polynomial of positive degree, we can write a in the form

$$(16) \quad a = \epsilon P_1^{e_1} \cdots P_n^{e_n},$$

where ϵ is in \mathbb{F}_q^{\times} , the P_i are distinct monic primes in A , and the e_i are positive integers. For each $1 \leq i \leq n$, set

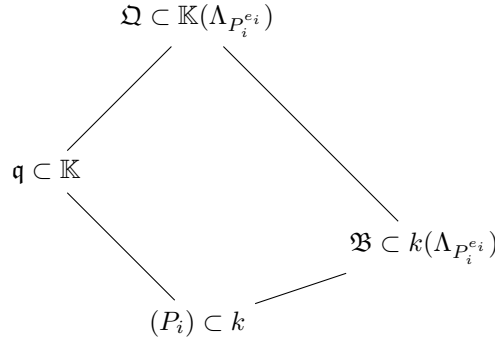
$$(17) \quad a_i := \frac{a}{P_i^{e_i}} \in A,$$

We prove that for each $1 \leq i \leq n$, there exists an element $b_i \in A$ with $\deg(b_i) < \deg(a)$ such that $C_{a_i}(C_{b_i}(\lambda_a) + h) \in \mathbb{K}$. Indeed, take an integer $1 \leq i \leq n$. Set

$$\Lambda_{P_i^{e_i}} = \{\gamma \in k^{\text{alg}} \mid C_{P_i^{e_i}}(\gamma) = 0\}.$$

We know from [9, Proposition 12.7] that $k(\Lambda_{P_i^{e_i}})$ is a Galois extension of k .

Let \mathfrak{q} be a prime of \mathbb{K} lying above $(P_i) = P_i A$, and let Ω be a prime of $\mathbb{K}(\Lambda_{P_i^{e_i}})$ lying above \mathfrak{q} . Let \mathfrak{B} be a prime of $k(\Lambda_{P_i^{e_i}})$ lying below Ω . Then \mathfrak{B} lies above (P_i) .



We prove that \mathfrak{q} is totally ramified in $\mathbb{K}(\Lambda_{P_i^{e_i}})$. Let $\mathbf{e}(\Omega/\mathfrak{q})$, $\mathbf{e}(\mathfrak{q}/(P_i))$ be the ramification indices of Ω over \mathfrak{q} and \mathfrak{q} over (P_i) , respectively. Let $\mathbf{e}(\Omega/\mathfrak{B})$, $\mathbf{e}(\mathfrak{B}/(P_i))$ be the ramification indices of Ω over \mathfrak{B} and \mathfrak{B} over (P_i) , respectively. Let $\mathbf{e}(\Omega/(P_i))$ be the ramification index of Ω over (P_i) . We know from

[9, Proposition 12.7] that the prime ideal $(P_i) = P_i A$ is totally ramified in the extension $k(\Lambda_{P_i^{e_i}})/k$, and thus

$$\mathbf{e}(\mathfrak{B}/(P_i)) = [k(\Lambda_{P_i^{e_i}}) : k] = \phi(P_i^{e_i}),$$

where $\phi(\cdot)$ denotes the function field analogue of the Euler ϕ -function (see, for example, [9, Proposition 1.7] for the definition of $\phi(\cdot)$). By assumption, we know that (P_i) is unramified in \mathbb{K} , and thus $\mathbf{e}(\mathfrak{q}/(P_i)) = 1$. Since $K(\Lambda_{P_i^{e_i}}) = K \cdot k(\Lambda_{P_i^{e_i}})$, it thus follows from [4, Lemma 4.6.3] that \mathfrak{B} is unramified in $\mathbb{K}(\Lambda_{P_i^{e_i}})$. Hence $\mathbf{e}(\mathfrak{Q}/\mathfrak{B}) = 1$, and we deduce that

$$(18) \quad \mathbf{e}(\mathfrak{Q}/\mathfrak{q}) = \mathbf{e}(\mathfrak{Q}/\mathfrak{q})\mathbf{e}(\mathfrak{q}/(P_i)) = \mathbf{e}(\mathfrak{Q}/(P_i)) = \mathbf{e}(\mathfrak{Q}/\mathfrak{B})\mathbf{e}(\mathfrak{B}/(P_i)) = \mathbf{e}(\mathfrak{B}/(P_i)) = \phi(P_i^{e_i}).$$

We contend that the degree of $\mathbb{K}(\Lambda_{P_i^{e_i}})$ over \mathbb{K} is less than or equal to $\phi(P_i^{e_i})$. Indeed, let χ be a primitive generator of $\Lambda_{P_i^{e_i}}$. We know from [12, Theorem 12.3.16] that χ is a root of the $P_i^{e_i}$ -th cyclotomic polynomial $\Phi_{P_i^{e_i}}(x) \in k[x] \subset \mathbb{K}[x]$ of degree $\phi(P_i^{e_i})$. Hence we deduce that

$$[\mathbb{K}(\Lambda_{P_i^{e_i}}) : \mathbb{K}] = [\mathbb{K}(\chi) : \mathbb{K}] \leq \deg(\Phi_{P_i^{e_i}}(x)) = \phi(P_i^{e_i}).$$

Therefore it follows from (18) that

$$\phi(P_i^{e_i}) = \mathbf{e}(\mathfrak{Q}/\mathfrak{q}) \leq [\mathbb{K}(\Lambda_{P_i^{e_i}}) : \mathbb{K}] \leq \phi(P_i^{e_i}),$$

and hence

$$\mathbf{e}(\mathfrak{Q}/\mathfrak{q}) = [\mathbb{K}(\Lambda_{P_i^{e_i}}) : \mathbb{K}] = \phi(P_i^{e_i}).$$

Thus \mathfrak{q} is totally ramified in $\mathbb{K}(\Lambda_{P_i^{e_i}})$.

We now consider the equation

$$(19) \quad C_{P_i^{e_i}}(z) = m.$$

Let \mathbb{L}_i be the splitting field of the polynomial $C_{P_i^{e_i}}(z) - m \in \mathbb{K}[z]$ over \mathbb{K} . Since the polynomial $C_{P_i^{e_i}}(z) - m$ is separable, we see that \mathbb{L}_i is a Galois extension of \mathbb{K} .

We prove that the equation given by (19) has a solution z_\wp in the completion \mathbb{K}_\wp for each prime $\wp \in \mathcal{H}$. Indeed take any prime $\wp \in \mathcal{H}$. We know that there exists an element x_\wp in \mathbb{K}_\wp such that $C_a(x_\wp) = m$. Since $a = P_i^{e_i} a_i$, we deduce that

$$(20) \quad C_{P_i^{e_i}}(C_{a_i}(x_\wp)) = C_{P_i^{e_i} a_i}(x_\wp) = C_a(x_\wp) = m.$$

Since $C_{a_i}(x) \in k[x] \subset \mathbb{K}[x]$ and $\mathbb{K} \subset \mathbb{K}_\wp$, we see that $C_{a_i}(x_\wp) \in \mathbb{K}_\wp$. Upon letting $z_\wp = C_{a_i}(x_\wp) \in \mathbb{K}_\wp$, we see from (20) that the equation $C_{P_i^{e_i}}(z) = m$ has a solution z_\wp in \mathbb{K}_\wp . Therefore the equation $C_{P_i^{e_i}}(z) = m$ has a solution z_\wp in the completion \mathbb{K}_\wp for each prime $\wp \in \mathcal{H}$. Applying Corollary 2.7 for the equation $C_{P_i^{e_i}}(z) = m$ with $P_i^{e_i}, m, \mathbb{L}_i, \chi$ in the roles of $a, m, \mathbb{L}, \lambda_a$, respectively, where we recall that χ is a primitive generator of $\Lambda_{P_i^{e_i}}$, we deduce that $\mathbb{L}_i = \mathbb{K}(\chi) = \mathbb{K}(\Lambda_{P_i^{e_i}})$, and thus

$$(21) \quad \text{Gal}(\mathbb{L}_i/\mathbb{K}) = \text{Gal}(\mathbb{K}(\Lambda_{P_i^{e_i}})/\mathbb{K}).$$

Recall that we have shown that \mathfrak{q} is totally ramified in $\mathbb{K}(\Lambda_{P_i^{e_i}})$ and the prime \mathfrak{Q} lies above \mathfrak{q} . Let $\mathcal{D}(\mathfrak{Q}/\mathfrak{q}) \leq \text{Gal}(\mathbb{K}(\Lambda_{P_i^{e_i}})/\mathbb{K})$ be the decomposition group of \mathfrak{Q} over \mathfrak{q} . Since \mathfrak{q} is totally ramified in $\mathbb{K}(\Lambda_{P_i^{e_i}})$, we deduce from (21) that

$$(22) \quad \mathcal{D}(\mathfrak{Q}/\mathfrak{q}) = \text{Gal}(\mathbb{K}(\Lambda_{P_i^{e_i}})/\mathbb{K}) = \text{Gal}(\mathbb{L}_i/\mathbb{K}).$$

By assumption (ii) in the statement of Theorem 3.1, there exists an element $x_\mathfrak{q}$ in the completion $\mathbb{K}_\mathfrak{q}$ such that $C_a(x_\mathfrak{q}) = m$. Hence $x_\mathfrak{q}$ belongs to the set \mathcal{S} , where \mathcal{S} is the set given by (1) in the proof of Theorem 2.2. Thus $x_\mathfrak{q} = C_{b_i}(\lambda_a) + h$ for some element $b_i \in A$ with $\deg(b_i) < \deg(a)$. We see that

$$C_{P_i^{e_i}}(C_{a_i}(x_\mathfrak{q})) = C_{P_i^{e_i} a_i}(x_\mathfrak{q}) = C_a(x_\mathfrak{q}) = m,$$

and thus $C_{a_i}(x_q)$ is a root of the polynomial $C_{P_i^{e_i}}(z) - m \in \mathbb{K}[z]$. Since $\mathbb{L}_i = \mathbb{K}(\Lambda_{P_i^{e_i}})$ is the splitting field of the polynomial $C_{P_i^{e_i}}(z) - m$ over \mathbb{K} , we deduce that

$$(23) \quad m_i := C_{a_i}(x_q) = C_{a_i}(C_{b_i}(\lambda_a) + h) \in \mathbb{K}_q \cap \mathbb{L}_i.$$

Since $\mathbb{K}_q \cap \mathbb{L}_i$ is the fixed field of $\mathcal{D}(\mathfrak{Q}/q)$ (see [6, Proposition 9.8]), we see from (23) that $\psi(m_i) = m_i$ for every $\psi \in \mathcal{D}(\mathfrak{Q}/q)$. By (22), we know that $\mathcal{D}(\mathfrak{Q}/q) = \text{Gal}(\mathbb{L}_i/\mathbb{K})$, and hence m_i belongs to \mathbb{K} .

In summary, we have shown that each $1 \leq i \leq n$, there exists an element $b_i \in A$ with $\deg(b_i) < \deg(a)$ such that $m_i = C_{a_i}(C_{b_i}(\lambda_a) + h) \in \mathbb{K}$.

Since the elements $P_i^{e_i}$ are pairwise coprime in the principal ideal domain A , it follows from the Chinese Remainder Theorem that there exists an element ϵ in A such that

$$(24) \quad \epsilon \equiv b_i \pmod{P_i^{e_i}}$$

for each $1 \leq i \leq n$. Set

$$(25) \quad x_{\mathbb{K}} := C_{\epsilon}(\lambda_a) + h.$$

We prove that $x_{\mathbb{K}}$ belongs to \mathbb{K} , and is a solution to the equation $C_a(x) = m$. We first show that $C_{a_i}(x_{\mathbb{K}}) = m_i$ for each $1 \leq i \leq n$.

Take any integer $1 \leq i \leq n$. By (24), there exists an element $\delta_i \in A$ such that $\epsilon = b_i + \delta_i P_i^{e_i}$. It thus follows from (25) and (17) that

$$\begin{aligned} C_{a_i}(x_{\mathbb{K}}) &= C_{a_i}(C_{\epsilon}(\lambda_a) + h) \\ &= C_{a_i}(C_{b_i + \delta_i P_i^{e_i}}(\lambda_a) + h) \\ &= C_{a_i}(C_{b_i}(\lambda_a) + h) + C_{a_i}(C_{\delta_i P_i^{e_i}}(\lambda_a)) \\ &= m_i + C_{\delta_i a_i P_i^{e_i}}(\lambda_a) \\ &= m_i + C_{\delta_i a}(\lambda_a) \\ &= m_i + C_{\delta_i}(C_a(\lambda_a)) \\ &= m_i. \end{aligned}$$

In particular, this implies that $C_{a_i}(x_{\mathbb{K}}) = m_i \in \mathbb{K}$ for every $1 \leq i \leq n$.

By (17), we deduce that $\gcd(a_1, a_2, \dots, a_n) = 1$, and thus there exist elements v_1, v_2, \dots, v_n in A such that

$$v_1 a_1 + v_2 a_2 + \dots + v_n a_n = 1.$$

Since $C_{v_i}(x) \in k[x] \subset \mathbb{K}[x]$ for every $1 \leq i \leq n$, we deduce that

$$x_{\mathbb{K}} = C_1(x_{\mathbb{K}}) = C_{v_1 a_1 + v_2 a_2 + \dots + v_n a_n}(x_{\mathbb{K}}) = C_{v_1}(C_{a_1}(x_{\mathbb{K}})) + \dots + C_{v_n}(C_{a_n}(x_{\mathbb{K}})) \in \mathbb{K}.$$

Furthermore since $m_1 = C_{a_1}(C_{b_1}(\lambda_a) + h)$ is a solution to the equation $C_{P_1^{e_1}}(z) = m$, we deduce that

$$C_a(x_{\mathbb{K}}) = C_{P_1^{e_1} a_1}(x_{\mathbb{K}}) = C_{P_1^{e_1}}(C_{a_1}(x_{\mathbb{K}})) = C_{P_1^{e_1}}(m_1) = m,$$

which proves that the equation $C_a(x) = m$ has a solution $x_{\mathbb{K}} \in \mathbb{K}$. Thus our contention follows. \square

Let $\mathcal{P}_{\mathbb{K}}$ be the set of all primes in \mathbb{K} . If \mathcal{H} is a set of primes of \mathbb{K} such that $\mathcal{P}_{\mathbb{K}} \setminus \mathcal{H}$ is finite and \mathcal{H} contains all primes of \mathbb{K} that divide a , then \mathcal{H} is of Dirichlet density 1. Hence we obtain the following result that is a special case of Theorem 3.1.

Corollary 3.2. *We maintain the same notation as in Theorem 2.2. Assume that \mathbb{K} is a Galois extension of k such that every prime P dividing a is unramified in \mathbb{K} . Then the equation $C_a(x) = m$ has a solution $x_{\mathbb{K}}$ in \mathbb{K} if and only if it has a solution x_{\wp} in the completion \mathbb{K}_{\wp} of \mathbb{K} for all primes $\wp \in \mathcal{H}$, where \mathcal{H} is a set of primes of \mathbb{K} such that $\mathcal{P}_{\mathbb{K}} \setminus \mathcal{H}$ is finite and \mathcal{H} contains all primes of \mathbb{K} that divide a .*

REFERENCES

- [1] L. CARLITZ, *A class of polynomials*, Trans. Amer. Math. Soc. **43** (1938), pp. 167–182.
- [2] D. GOSS, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (**3**) [Results in Mathematics and Related Areas (**3**)], **35**, Springer-Verlag, Berlin, (1996).
- [3] D.R. HAYES, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), pp. 77–91.
- [4] H. KOCH, *Number Theory*, Algebraic numbers and functions. Translated from the 1997 German original by David Kramer. Graduate Studies in Mathematics, **24**. American Mathematical Society, Providence, RI, (2000).
- [5] J.S. MILNE, *Class Field Theory*, Available at <http://www.jmilne.org/math/CourseNotes/CFT.pdf>.
- [6] J. NEUKIRCH, *Algebraic number theory*, Translated from the 1992 German original and with a note by Norbert Schapacher. With a foreword by G. Harder. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], **322**. Springer-Verlag, Berlin, (1999).
- [7] T. ONO AND T. TERASOMA, *On Hasse principle for $x^n = a$* , Proc. Japan Acad. Ser. A Math. Sci. **73** (1997), no. **7**, 143–144.
- [8] T. ONO, *A note on Shafarevich–Tate sets for finite groups*, Proc. Japan Acad. Ser. A Math. Sci. **74** (1998), no. **5**, 77–79.
- [9] M. ROSEN, *Number theory in function fields*, Graduate Texts in Mathematics, **210**. Springer-Verlag, New York (2002).
- [10] D.S. THAKUR, *Function Field Arithmetic*, World Scientific Publishing Co., Inc., River Edge, NJ, (2004).
- [11] G.-J. VAN DER HEIDEN, *Local-global problem for Drinfeld modules*, J. Number Theory **104** (2004), no. **2**, 193–209.
- [12] G.D. VILLA SALVADOR, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA (2006).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BRITISH COLUMBIA, V6T 1Z2, CANADA

E-mail address: dongquan.ngoc.nguyen@gmail.com